Amendments to the Claims

Please make the following amendments to the Claims:

1. (Currently Amended) A method for facilitating secure data communications using a secret key for encrypting data flowing between first computing node comprising a processor and a memory and second computing node ~~comprising a processor and a memory~~ over a communications link, the method comprising:

determining that the communications link has been idle for at least a predetermined period of time ~~is idle~~, the communications link intermittently fluctuating between idle and busy, the idle communication link having no secure data transmission within the at least a predetermined period of time ~~in response to detecting that a heartbeat flowed across the communications link~~;

determining that there is data to flow over the idle communications link between the first computing node and the second computing node; and

generating a new secret key on demand exclusively in response ~~responsive~~ to determining that there is data to flow over the ~~previously~~ idle communications link and in response to determining that the communication link ~~is~~ has been idle for at least the predetermined period of time, ~~initiating generation of a new secret key,~~ the new secret key for encrypting data sent between the first computing node and the second computing node over the communications link.

2-38. (Canceled)

39. (Currently Amended) A method performed at a first computing node comprising a processor and a memory for facilitating secure data communications by using a secret key for encrypting data flowing between said first computing node and a second computing node ~~comprising a processor and a memory~~ over a communications link, the method comprising [[the]]:

determining that the communications link has been idle for at least a predetermined period of time ~~is idle~~, the communications link intermittently fluctuating between idle and busy, the idle communication link having no secure data transmission within the at least a predetermined period of time ~~in response to detecting that a heartbeat flowed across the communications link~~;

determining that data is available for flow over the idle communications link between the first computing node and the second computing node; and

generating a new secret key on demand before transmission over the idle communications link recommences, in response to a determination that data is available and a determination that the communications link ~~is~~ has been idle for at least the predetermined period of time, ~~initiating generation of a~~ the new secret key for use in encoding at least part of the

available data before the available data flows onto the communications link.

40. (Cancelled).

41. (Currently Amended) The method of ~~either~~ claim 39 ~~or claim 40~~ including the additional steps of:

determining whether the amount of data sent over the communications link since the last generation of a secret key exceeds a predetermined amount threshold; and

if the amount of data sent exceeds the predetermined amount threshold, initiating generation of a new secret key.

42. (Currently Amended) The method of claim ~~40~~ 39 including the additional steps of:

sending a heartbeat message to the second computing node only if it is determined that the link has been idle for at least the predetermined period of time and that there is no data available for flow over the communications link; and

monitoring the communications link for receipt of an acknowledgement from the second computing node.

43. (Currently Amended) The method of claim 42 including the additional step of terminating the communications link with the second computing node if no acknowledgement is received from the second computing node within a predetermined period of time.

44. (Currently Amended) An apparatus for facilitating secure data communications by using a secret key to encrypt data flowing over a communications link between the apparatus and a remote system, said apparatus comprising:

a data detector for determining whether the communications link has been idle for at least a predetermined period of time using a timer ~~is idle~~, the communications link intermittently fluctuating between idle and busy, the idle communication link having no secure data transmission within the at least a predetermined period of time ~~in response to detecting that a heartbeat flowed across the communications link~~, the data detector determining that data is now available for flow to the remote system over the communications link;

key generation logic for generating a new secret key on demand in response ~~responsive~~ to determinations that the communications link has been idle for at least the predetermined period of time and there is data now available for flow to the remote system, ~~to initiate generation of a~~ the new secret key for use in encoding at least part of the available data before the available data flows onto the communications link; and

a byte measurer for determining whether the amount of data sent over the communications link has exceeded a predetermined amount threshold since the last generation of a secret key and

wherein the key generation logic initiates generation of a new secret key if the determination is that the amount of data sent has exceeded the predetermined amount threshold.

45. (Cancelled).

46. (Cancelled).

47. (Currently Amended) The apparatus of claim [[46]] 44 further including a heartbeat issuer for sending a heartbeat to the remote system if the data detector determines that the communications link has been idle but there is no data available for flow to the remote system over the communications link.

48. (Original) The apparatus of claim 47 further including a detector for monitoring the communications link for an acknowledgment of the heartbeat from the remote system.

49. (Original) The apparatus of claim 48 further including a connection terminator for terminating the communications link if the detector fails to detect an acknowledgment of the heartbeat from the remote system within the predetermined period of time.

50. (Currently Amended) A program product comprising a computer readable storage media embodying program instructions executed by a computer to facilitate secure data

communications with a remote system by using a secret key for encrypting data flowing between the computer and the remote system over a communications link by:

determining that the communications link has been idle for at least a predetermined period of time ~~is idle~~, the communications link intermittently fluctuating between idle and busy, the idle communication link having no secure data communication traffic within the at least a predetermined period of time;

sending a heartbeat message to the remote system only if it is determined that the link has been idle for at least a predetermined period of time and that there is no data available for flow over the communications link;

monitoring the communications link for receipt of an acknowledgement from the remote system;

receiving the acknowledgement from the remote system within a predetermined period of time;

determining that data is available for flow over the idle communications link from the computer to the remote system;

detecting that a heartbeat flowed across the idle communications link; and

generating a new secret key on demand exclusively ~~only~~ in response to a determination that data is available for flow over the idle communications link, detecting that a heartbeat flowed across the idle communications link, and receiving the acknowledgement from the remote system within the

predetermined period of time, ~~initiating generation of a~~ the new secret key for use in encoding at least part of the available data before the available data flows onto the communications link, such that generation of a new secret key exclusively occurs when data is available for flow over the idle communications link.

51. (Currently Amended) The program product of claim 50 further including program instructions ~~for determining whether the communications link has been idle for at least a predetermined period of time and~~ for generating a new secret key only if the communications link is found to have been idle for at least the predetermined period of time.

52. (Original) The program product of either claim 50 or claim 51 including additional program instructions for:

determining whether the amount of data sent over the communications link since the last generation of a secret key exceeds a predetermined amount threshold; and

initiating generation of a new secret key if the amount of data sent is determined to have exceeded the predetermined amount threshold.

53. (Cancelled).

54. (Previously Presented) The program product of claim 50 including an additional program instruction for terminating the communications link with the remote system if no acknowledgement is received from the remote system within the predetermined period of time.